VILE S	Δ		~	• • •
mne n				
MAR 2 0 2001	ଥି		Approved for u	
e S	Ander the Panerwork Reduction Act of 19	05 no nersons are required to reson	U.S. Patent and Trademark Office: and to a collection of information unless	

PTO/SB/08A (08-00)

MYX		Approved for use through 10/31/2002 OMB 0651-0031 U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE				
		nder the Paperwork Reduction Act of 1995, no persons are requ			ımber	
Substitute for Form 1449/A/PTO			Complete if Known			
Supstitute i	ior Politi	1449/AP-10	Application Numb r	09/654,638		
1	INFC	DRMATION DISCLOSURE	Filing Date	September 5, 2000		
			First Named Inventor	Tsuyoshi, Takagi		
,	<b>51A</b>	TEMENT BY APPLICANT	Group Art Unit	T Be Assigned		
		(use as many sheets as necessary	Examiner Name	To Be Assigned		
Sheet	1	of 1	Attorney Docket Number	13700-0251 (KS#44471/23405	55)	
	·		ATENT LITERATURE DOCUME			
Examiner Initials	Cite No.¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published				
	1 HUHNLEIN; A Cryptosystem Based On Non-Maximal Imaginary Quadratic Orders With Fast Decryption; ADVANCE					
MD		CRYPTOLOGY-EUROCRYPT '98, 1998, PGS 294-3	07	ι	ľ	
0	2	MENEZES: Handbook of Applied Cryptography, 1997	7, CRC Press, Boca Raton, Florid	a 33431		
Mp				*		
-	187				·	
	3	BUCHMANN; On the Complexity and Efficiency of a	New Key Exchange System; ADV	ANCES IN CRYPTOLOGY -		
MD		EUROCRYPT '89; 1990, pgs 597-616			1/	
		a calculation				
	4	BIEHL; Cryptographic Protocols Based on Discrete L	ogarithms in Real-Quadratic Orde	ers; ADVANCES IN CRYPTOLOGY -		
MO		CRYPTO '94, 1994, pgs. 56-60			** **	
		entragement of the first party of	· · · · · · · · · · · · · · · · · · ·			
	5	RIVEST; Obtaining Digital Signatures and Public-Key	Cryptosystems Communications	of the ACM, Feb. 1978, Vol. 21, #2,		
MD)		pgs. 120-126.				
• •					ľ	
	6	CHAUM; Centre for Mathematics and Computer Scie.	nce, 1998, Springer-Verlag, pgs.	212-214.		
MD		·				
' (1)		**				
	7	GENNARO; RSA-Based Undeniable Signatures; 199	8. Springer-Verlag, pgs. 132, 149			
140			3.75			
MD						
	8	SHANKS; On Gauss and Composition 1, NUMBER T	THEORY AND APPLICATIONS A	ne 163.204 1080 Kluwer Academia	<b></b>	
^			HEORI AND AFTERMIONS, P	ys. 103°204, 1303, Niuwel Acadelnic		
MI)	1	Publishers		•	-	
	<del>  -</del>	A Companyator Paged on Non-Atomical Inc.	Number of the Contract of the		,1 1	
h 4×0	9	A Cryptosystem Based on Non-Maximal Imaginary Q	uadratic Orders with Fast Decryp	tion; Proceedings Eurocrypt '98; March		
MD		1998, pgs. 294-307.		*		
d ain	10	Conference on the Mathematics of Public Key Crypto	ography, June 12, 1999, pgs 1-17			
MD		0				
				* *		
		-		REOF.		
	1.	( · · · · · · · · · · · · · · · · · · ·		'IECEIVED	ĺ	
				MAD	ĺ	
				RECEIVED  MAR 2 2 7001		
				Technology Center 2100		
	1			Centar 2400		

Examiner		Date	\$ 14/04
Signature	Must Suf	Considered	1-7.70

<sup>&</sup>lt;sup>1</sup>Unique citation designation number. <sup>2</sup>Applicant is to place a check mark here if English language translation is attached.